Flight Projects
Directorate
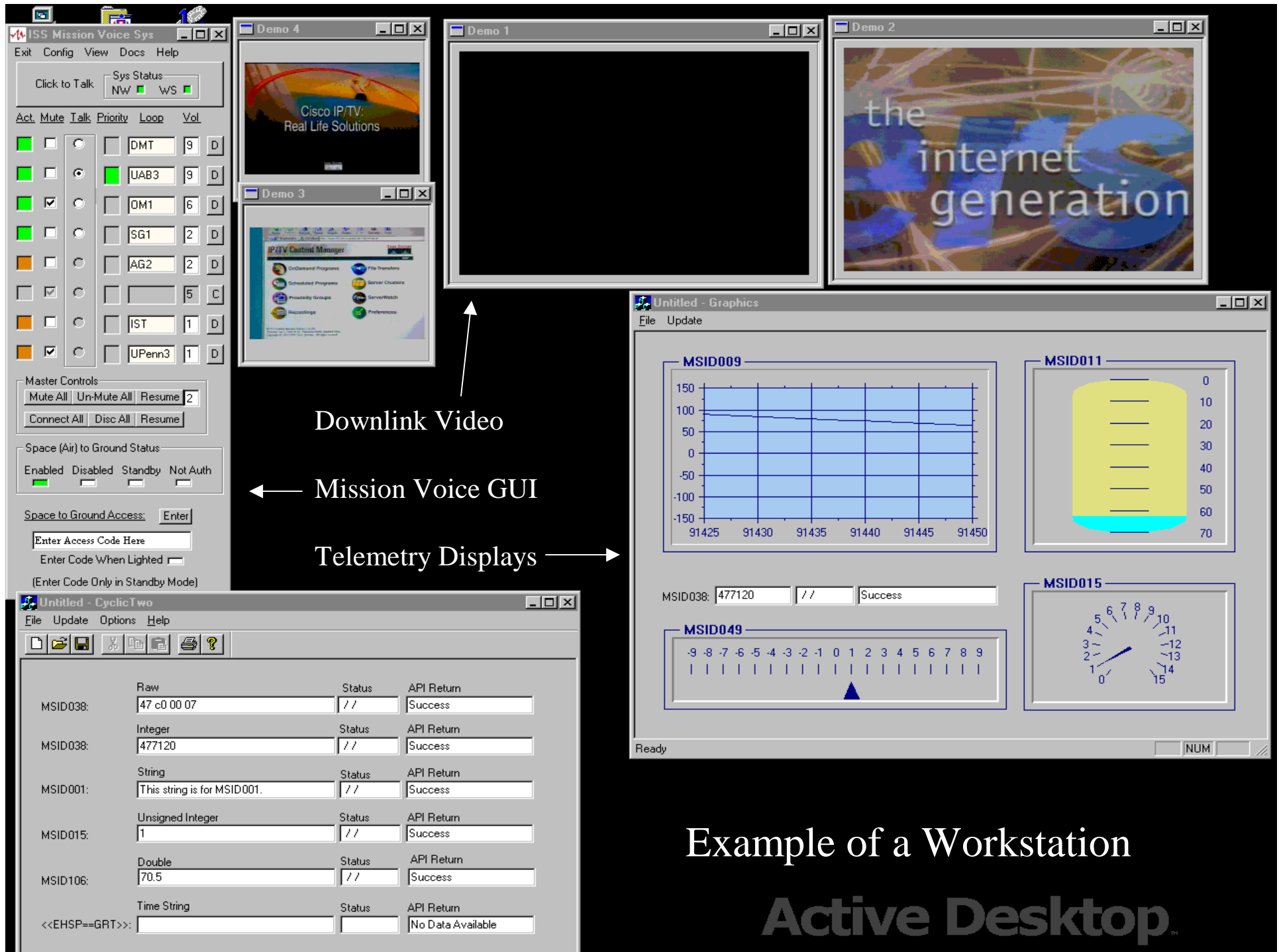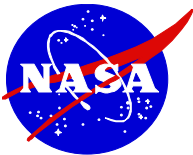
ISS REMOTE OPS OVERVIEW

NETWORKING & DOWNLINK VIDEO
VOICE
END USER PLATFORM
SECURITY OVERVIEW

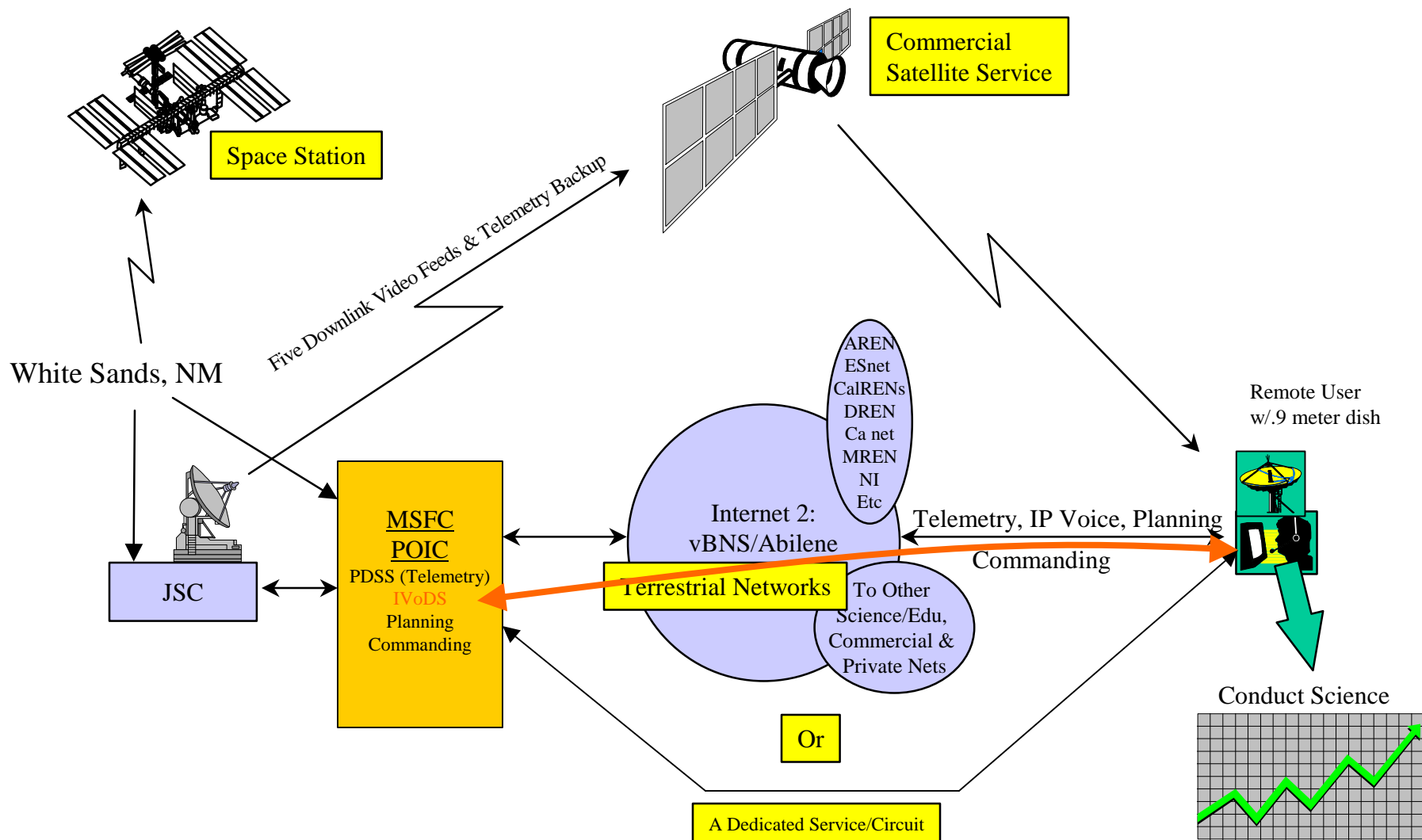Note: Information contained in this presentation is subject to change

ISS Mission Voice Sys

Exit   Config   View   Docs   Help

Click to Talk

Sys Status
NW   WS

Act. Mute Talk Priority Loop Vol

DMT 9 D
UAB3 9 D
OM1 6 D
SG1 2 D
AG2 2 D
5 C
IST 1 D
UPenn3 1 D

Master Controls
Mute All Un-Mute All Resume 2
Connect All Disc All Resume

Space (Air) to Ground Status
Enabled Disabled Standby Not Auth

Space to Ground Access: Enter
Enter Access Code Here
Enter Code When Lighted
(Enter Code Only in Standby Mode)

Demo 4
Cisco IP/TV:
Real Life Solutions

Demo 3
IP/TV Content Manager
OnDemand Programs   File Transfers
Scheduled Programs   Server Clusters
Proximity Groups   ServerWatch
Recordings   Preferences

Demo 1

Demo 2
the internet generation

Downlink Video

Mission Voice GUI

Telemetry Displays

Untitled - Graphics
File   Update

MSID009
150
100
50
0
-50
-100
-150
91425 91430 91435 91440 91445 91450

MSID038: 477120 / / Success

MSID049
-9 -8 -7 -6 -5 -4 -3 -2 -1 0 1 2 3 4 5 6 7 8 9

MSID011
0
10
20
30
40
50
60
70

MSID015

Ready   NUM

Untitled - CyclicTwo
File   Update   Options   Help

	Raw	Status	API Return
MSID038:	47 c0 00 07	/ /	Success

	Integer	Status	API Return
MSID038:	477120	/ /	Success

	String	Status	API Return
MSID001:	This string is for MSID001.	/ /	Success

	Unsigned Integer	Status	API Return
MSID015:	1	/ /	Success

	Double	Status	API Return
MSID106:	70.5	/ /	Success

	Time String	Status	API Return
<<EHSP==GRT>>:			No Data Available

Example of a Workstation

Active Desktop

ISS TO SCIENCE USER END TO END CONNECTIVITY

POIC to END USER CONFIGURATION

POIC

Abilene or vBNS Networks

User Workstation(s)

Backup

POIC Systems
PDSS (Telemetry)
IVoDS (Voice)
Command
PPS (Planning)

Science Nets

FIREWALL

User Mission LAN

Comm I/F	Functions	HW Req'd	SW Req'd	Security
MPEG II	Downlink Video (5)	Receiver Card	Viewer Client	Controlled Inputs
UDP/IP	Telemetry Processing and Display	Network Interface Card	TReK SW	User Provided
IP Stack	Payload Voice	Sound Card, & Headset	Browser & Plug In	VPN Client
TCP/IP	Payload Planning Data	None	Browser	Secure Socket Layer
	Payload Commanding	None	Hummingbird Exceed	Secure Shell

IVoDS Requirement Summary

- Phase I Voice Functions
  - Monitor 8 loops simultaneously
  - Talk on one loop of these eight loops
  - Talk on Space (Air) to Ground, if enabled
  - Volume control and mute for individual loops
  - Differentiate between talk and monitor privileges
  - Show lighted talk traffic per loop
  - System management through admin and PAYCOM clients
  - 30 minute server restoration time
- Capacity: Initial deployment 200 simultaneous users, up to 1600 flows
- Security

IVoDS User Client Functional Example

(Includes Phase One and Phase Two)

Note: This is an example only. The operational client may be different both visually and functionally

Attached Payload Telecon

Payload User/Developer Considerations/Recommendations

1. Use TReK for telemetry processing (available in July) and commanding (available 3/01)
2. Use IVoDS to connect to the POIC mission voice system
3. Use a dedicated mission LAN and interface to an Internet 2 network (vBNS or Abilene) instead of sharing with admin or other traffic
4. Develop/design an operational plan (determine workstation performance demands)
5. Develop a mission traffic/data flow plan, end to end if possible
   - Data modes, i.e. realtime, playback, dump
6. PDSS delivers realtime telemetry at the downlinked native rate
   - i.e. realtime payload to ground =1Mb then PDSS to a user =1Mb
   - Buffering is generally not provided
7. Data rate is additive: realtime rate+x data mode rates=ingress data rate
8. Firewall considerations
   - Location and policies
   - UDP, HTTP and FTP
   - Will require all these and TCP

Payload User/Developer Considerations/Recommendations (Cont)

9. Fully implement the security requirements/guidelines in the PGUIDD to protect the POIC systems and your systems

10. Be security aware!

11. Implement a downlink video terminal, even if you have no downlink video requirements, for the "best effort" telemetry backup feature of the downlink video service

> Cost is less than $1K with <u>no</u> recurring or monthly charges

> Video service available 12/00

12. Protection of a user's data is a user responsibility, telemetry streams are not protected by the POIC over LANs or WANs

13. Downlink video hardware and software including the dish required is not known until a vendor has been selected

> Broadlogic MPEG II PCI card is an example of a PCI based interface

Voice Security Approach

- Security Related Highlights
  - Security guidelines specified in the PGUIDD are implemented at the user site
    - Requires development of a security plan
    - Security commensurate to your operational plan
  - Loop access requires pre-approval and individual loop privileges assigned by the GSRT
  - Loop access approved by the owner or their designee
  - Loop access, password and other sensitive access information encrypted for storage on IVoDS admin and user platforms
  - IVoDS initial authentication will use digital certificates
  - Virtual Private Network (VPN) using 3DES
  - User must logon to IVoDS separate from the VPN
  - Admin database to include user specific local telephone and contact information
  - PAYCOM position or IVoDS administrator can eliminate entire loops or an individual(s) from a single loop
  - Use of static IP addresses
  - User client software plug in downloaded from secure POIC web site

Attached Payload Telecon

(6/8/00)

Digital Certificate Authentication and VPN Initiation Process
No Network Security Present
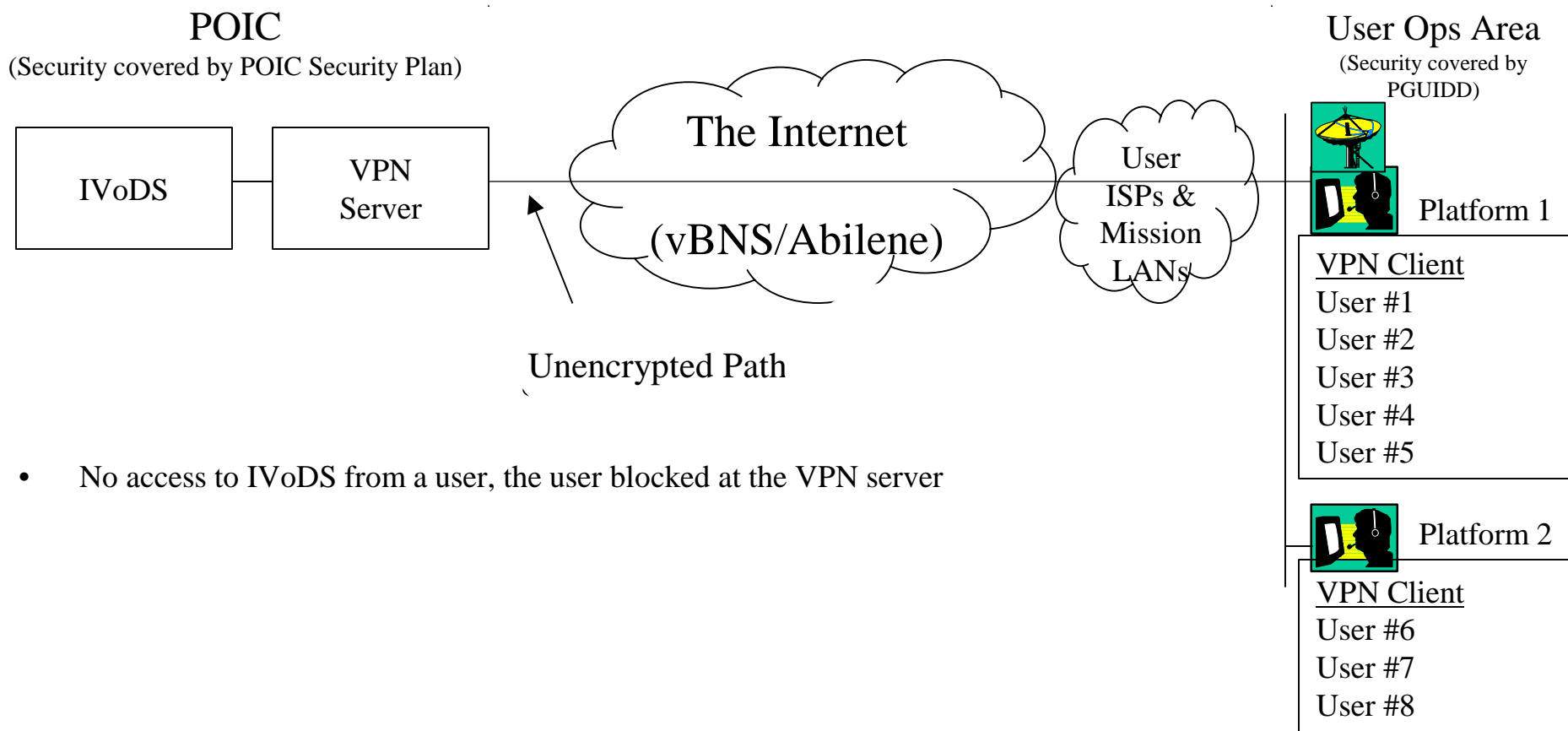
POIC
(Security covered by POIC Security Plan)

User Ops Area
(Security covered by PGUIDD)

IVoDS — VPN Server

The Internet

(vBNS/Abilene)

User ISPs & Mission LANs

Platform 1

VPN Client
User #1
User #2
User #3
User #4
User #5

Platform 2

VPN Client
User #6
User #7
User #8

Unencrypted Path

- No access to IVoDS from a user, the user blocked at the VPN server

Attached Payload Telecon

(6/8/00)

Digital Certificate Authentication and VPN Initiation Process (Cont)
Digital Certificate Handshaking & 3DES Key Exchange
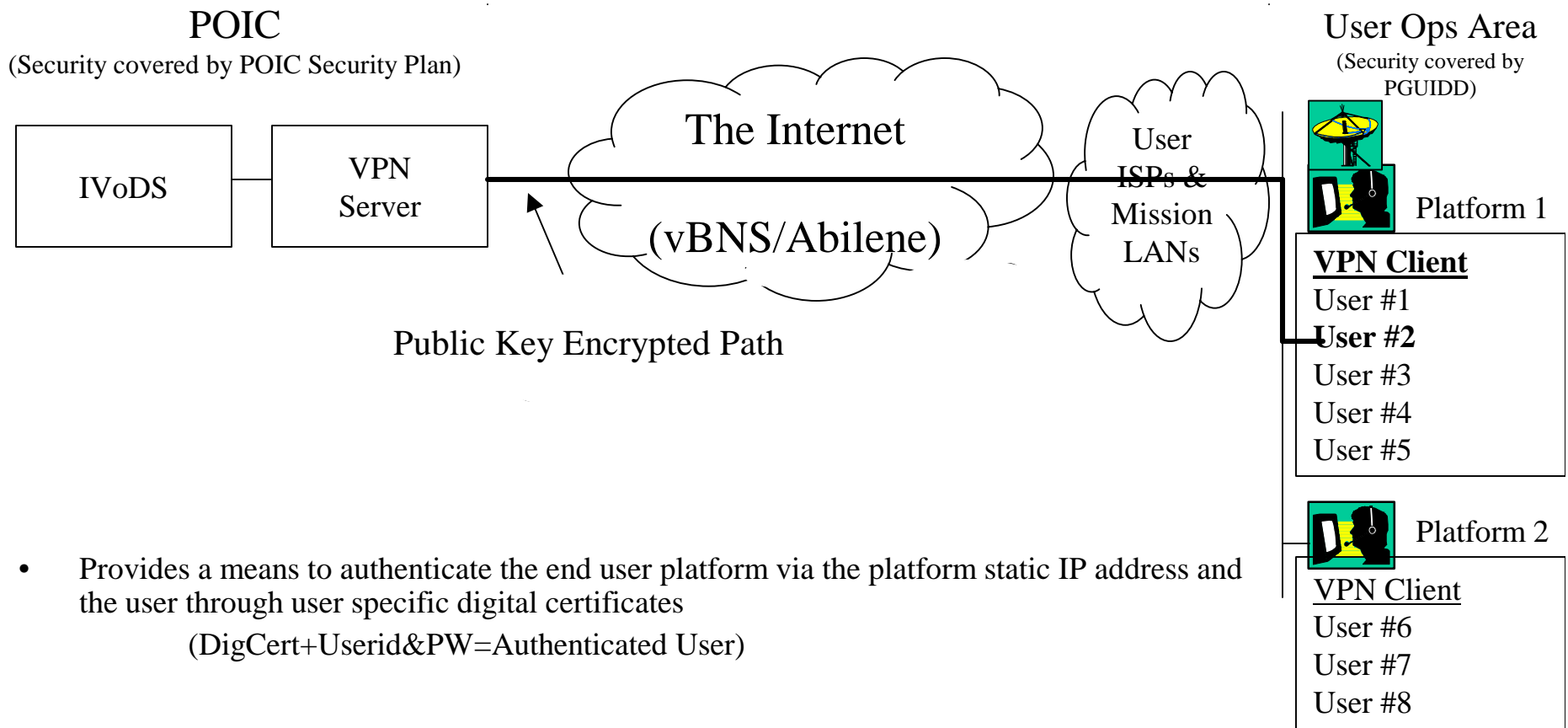
POIC
(Security covered by POIC Security Plan)

User Ops Area
(Security covered by PGUIDD)

IVoDS

VPN Server

The Internet

(vBNS/Abilene)

User ISPs & Mission LANs

Platform 1

VPN Client
User #1
User #2
User #3
User #4
User #5

Platform 2

VPN Client
User #6
User #7
User #8

Public Key Encrypted Path

- Provides a means to authenticate the end user platform via the platform static IP address and the user through user specific digital certificates

  (DigCert+Userid&PW=Authenticated User)

Digital Certificate Authentication and VPN Initiation Process (Cont)
VPN Protection

POIC
(Security covered by POIC Security Plan)

User Ops Area
(Security covered by PGUIDD)

| IVoDS | | VPN Server |

The Internet

(vBNS/Abilene)

User ISPs & Mission LANs

Platform 1

Platform 2

Platform 3

3DES Encrypted Path °
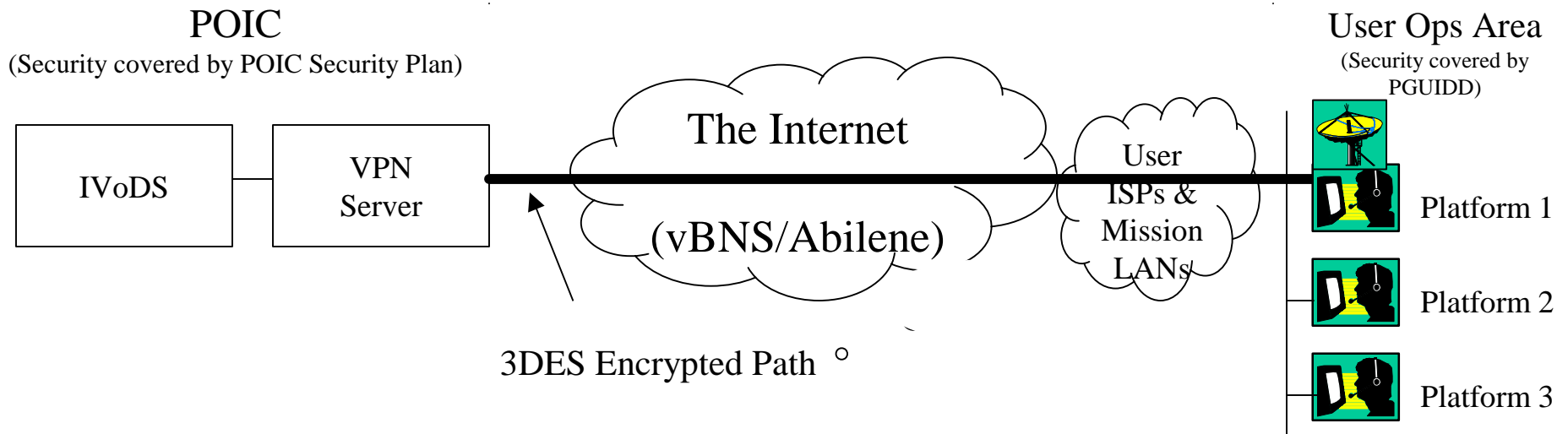
- Protect against IP spoofing
- Provide confidentiality over the Internet from the VPN server to the user's platform
- User identification and individual packet authentication
- Use 3DES encryption

Attached Payload Telecon

(6/8/00)

Digital Certificate Authentication and VPN Initiation Process (Cont)
IVoDS Logon
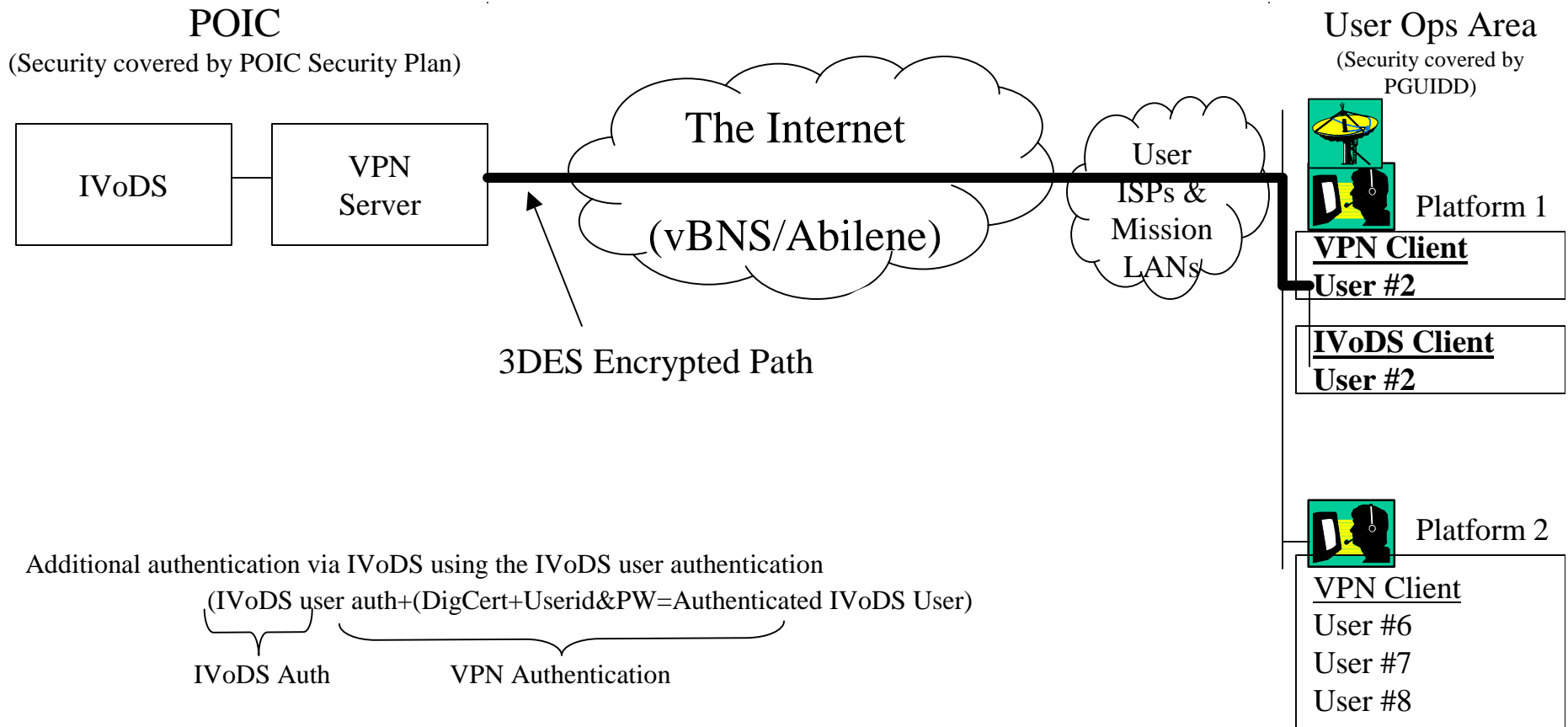
POIC
(Security covered by POIC Security Plan)

IVoDS		VPN Server

The Internet

(vBNS/Abilene)

User ISPs & Mission LANs

User Ops Area
(Security covered by PGUIDD)

Platform 1

VPN Client
User #2

IVoDS Client
User #2

3DES Encrypted Path

Platform 2

VPN Client
User #6
User #7
User #8

- Additional authentication via IVoDS using the IVoDS user authentication

(IVoDS user auth+(DigCert+Userid&PW=Authenticated IVoDS User)

IVoDS Auth   VPN Authentication

Attached Payload Telecon

(6/8/00)

Digital Certificate Authentication and VPN Initiation Process (Cont)
Space (Air) to Ground Enabling

POIC
(Security covered by POIC Security Plan)

User Ops Area
(Security covered by PGUIDD)

The Internet

(vBNS/Abilene)

User ISPs & Mission LANs

IVoDS — VPN Server

Platform 1

VPN Client
User #2

IVoDS Client
User #2

3DES Encrypted Path

PAYCOM Position

Admin Client To Enable S/G for User #2	Voice Authentication with User #2

Platform 2

VPN Client
User #6
User #7
User #8

- PAYCOM client enable the S/G IVoDS conference for Platform 1 User #2 using VPN path
- Authentication already provided through logon and real time person to person voice via the PAYCOM loop
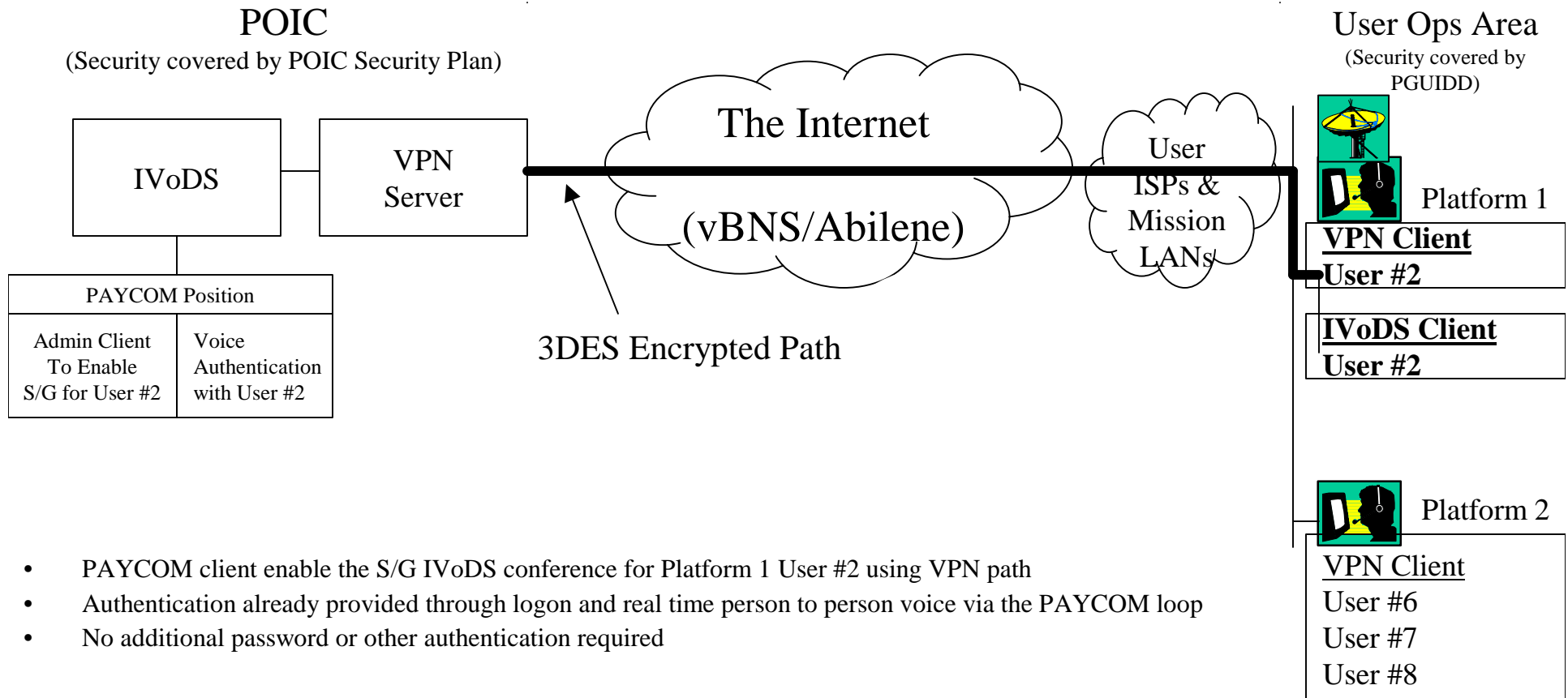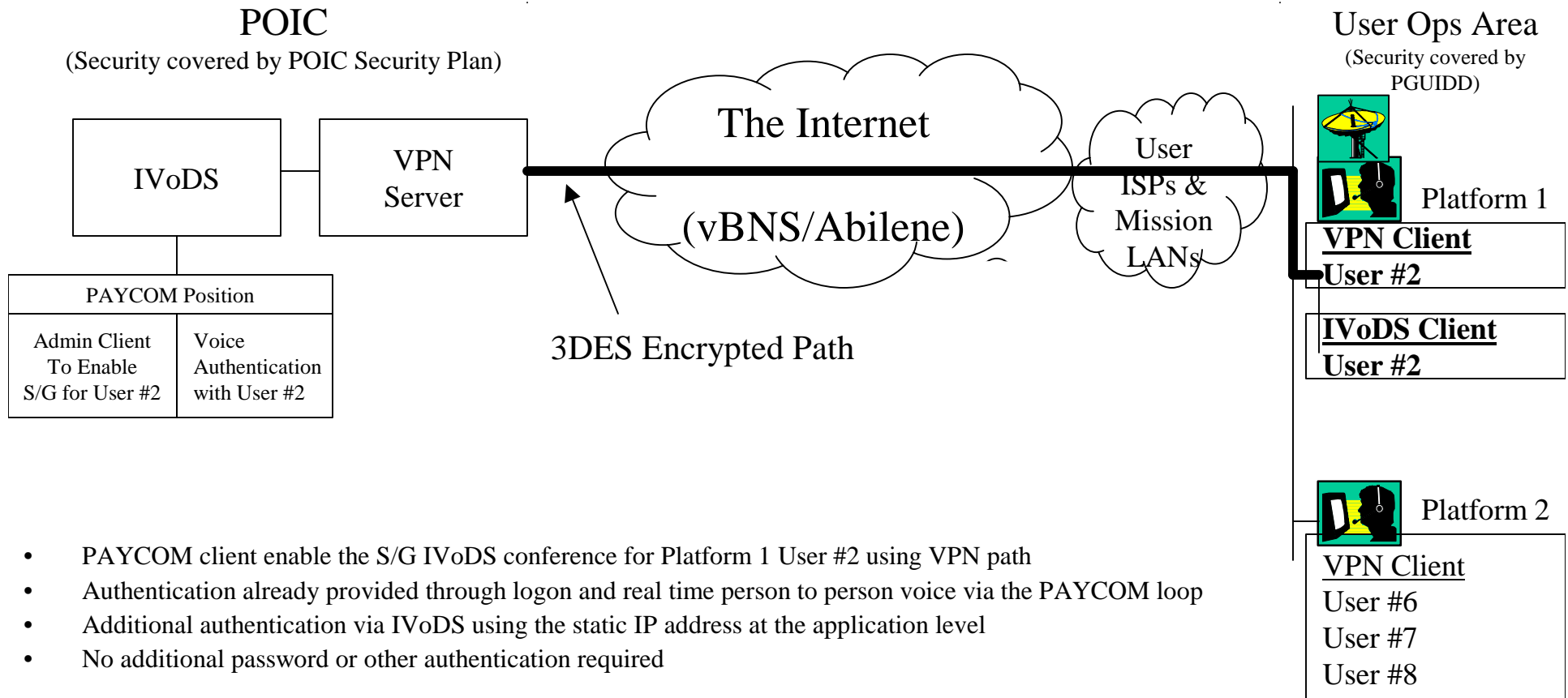- No additional password or other authentication required

Attached Payload Telecon

(6/8/00)

Digital Certificate Authentication and VPN Initiation Process (Cont)
Space (Air) to Ground Interface

POIC
(Security covered by POIC Security Plan)

User Ops Area
(Security covered by PGUIDD)


```
IVoDS ─── VPN Server ─── The Internet (vBNS/Abilene) ─── User ISPs & Mission LANs
```

3DES Encrypted Path

PAYCOM Position

| Admin Client To Enable S/G for User #2 | Voice Authentication with User #2 |

Platform 1

VPN Client
User #2

IVoDS Client
User #2

Platform 2

VPN Client
User #6
User #7
User #8

- PAYCOM client enable the S/G IVoDS conference for Platform 1 User #2 using VPN path
- Authentication already provided through logon and real time person to person voice via the PAYCOM loop
- Additional authentication via IVoDS using the static IP address at the application level
- No additional password or other authentication required

Technical Contacts

- TReK: Telemetry and Commanding – Michele Schneider, 256-544-1535

- Internet Voice, Downlink Video and Network Connectivity - Bob Bradford, 256-544-2843

- Planning – Theresa Maxwell, 256-544-2232

- Security – Pattie Sanderson, 256-544-3803

- Get the Process Started:
    - Nick Bornas, 256-544-5235